

CLAIMS

5 We claim:

1. A method for authenticating a digital medium comprising:
monitoring a transfer rate of read data resulting from the reading of valid data
stored on a digital medium at a physical location;
determining, from the monitored transfer rate, the presence of an anomaly region
on the digital medium corresponding to the physical location of the valid data on the
digital medium; and
authenticating the digital medium based on a characteristic of the anomaly region.
2. The method of claim 1 wherein the digital medium comprises an optical digital medium.
3. The method of claim 1 wherein the digital medium comprises a magnetic digital medium.
4. The method of claim 1 wherein monitoring comprises monitoring the transfer rate in real
time, as the read data is read from the digital medium.
5. The method of claim 1 wherein monitoring comprises monitoring the transfer rate
following reading of the read data from the digital medium.
6. The method of claim 1 further comprising estimating the monitored data transfer rate and
determining the presence of the anomaly region based on the estimated data transfer rate.
7. The method of claim 1 wherein the anomaly region causes a modification in the transfer
rate of the read data.

8. The method of claim 7 wherein the reading of the valid data is performed by a reading device and wherein the modification in the transfer rate results from the reading device automatically initiating multiple retries of reading the valid data due the presence of the anomaly region.
9. The method of claim 7 wherein the reading of the valid data is performed by a reading device and wherein the modification in the transfer rate results from the reading device automatically slowing down the reading the valid data due the presence of the anomaly region.
10. The method of claim 1 wherein the anomaly region is located at a predetermined location on the medium.
11. The method of claim 10 wherein the predetermined location comprises an absolute address on the medium.
12. The method of claim 11 wherein the absolute address represents an encoded data value.
13. The method of claim 1 wherein the anomaly region is at a location on the medium that is analytically determined as a result of the step of determining the presence of the anomaly region.
14. The method of claim 13 wherein the predetermined location comprises an absolute address on the medium.
15. The method of claim 14 wherein the absolute address represents an encoded data value.
16. The method of claim 1 wherein the anomaly region comprises a first anomaly region and further comprising:

determining, from the monitored transfer rate, the presence of a second anomaly region on the digital medium corresponding to a second physical location of second valid data on the digital medium; and

wherein a relative location of the second anomaly region is determined relative to the location of first anomaly region.

17. The method of claim 16 wherein authenticating is further based on the determined relative location.
18. The method of claim 16 wherein the second anomaly region is located at a predetermined location on the medium.
19. The method of claim 16 wherein the second anomaly region is at a location on the medium that is analytically determined as a result of the step of determining the presence of the second anomaly region.
20. The method of claim 16 wherein the relative location represents an encoded data value.
21. The method of claim 1 wherein the characteristic is the location of the anomaly region in the read data, and wherein if the location of the anomaly region in the read data matches the physical location of the anomaly region corresponding to the valid data, then the digital medium is determined as authentic.
22. The method of claim 21 wherein if the location of the anomaly region in the read data does not match the physical location of the anomaly region corresponding to the valid data, then the digital medium is determined as non-authentic.
23. The method of claim 1 further comprising controlling user access to the valid data on the digital medium based on whether the medium is authentic.

24. The method of claim 23 wherein controlling comprises one of allowing access, disallowing access, and limiting access to the valid data on the digital medium.
25. The method of claim 1 wherein the determination of the presence of the anomaly region results from a difficulty in the reading of the read data by a reading device.
26. The method of claim 1 wherein the anomaly region comprises a physical alteration of the digital medium that results in the valid data corresponding to the anomaly region being readable at a transfer rate that is different than a standard transfer rate of valid data not corresponding to the anomaly region.
27. The method of claim 26 wherein the physical alteration of the digital medium comprises a mechanical alteration.
28. The method of claim 26 wherein the physical alteration of the digital medium comprises an optical alteration.
29. The method of claim 26 wherein the physical alteration of the digital medium comprises a magnetic alteration.
30. The method of claim 1 wherein the steps for performing the authentication reside in software code that is previously stored on the digital medium, prior to authentication.
31. The method of claim 1 wherein the steps for performing the authentication reside in firmware that is stored in a media drive performing the authentication or in a computing device controlling the media drive, or stored in firmware controlling the media drive, or stored remotely and provided to the media drive by a network connection.
32. The method of claim 1 wherein a known characteristic of the anomaly region is previously stored, prior to authentication, and wherein authenticating the digital medium

based on a characteristic of the anomaly region comprises comparing the characteristic to the known characteristic.

- 5
33. The method of claim 1 wherein the presence of the anomaly region is determined according to a modification in the transfer rate of the read data.
34. The method of claim 33 wherein the modification in the transfer rate comprises a reduction in the transfer rate and wherein the anomaly region is identified based on the extent of the reduction.
35. The method of claim 33 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant non-zero transfer rate.
36. The method of claim 35 wherein the resultant non-zero transfer rate results in a determination that the anomaly region is a genuine anomaly region.
37. The method of claim 33 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant zero transfer rate.
- 20 38. The method of claim 37 wherein the resultant zero transfer rate results in a determination that the anomaly region is a false anomaly region
39. The method of claim 38 wherein the false anomaly region indicates that the digital medium is non-authentic.
- 25
40. The method of claim 33 wherein the modification in the transfer rate comprises an increase in the transfer rate, and wherein the characteristic is determined based on the increase.

41. The method of claim 33 wherein the modification in the transfer rate comprises a response comprising an acceptable reduction in the data transfer rate followed by a sudden increase in the transfer rate to an increased transfer rate that is greater than a maximum transfer rate.
42. The method of claim 41 wherein the response indicates that an apparent anomaly region generated by an external source has been detected.
43. The method of claim 42 further comprising filtering the apparent anomaly region such that authenticating is not based on the apparent anomaly region.
44. The method of claim 1 wherein authenticating is based on a characteristic of multiple anomaly regions.
45. The method of claim 1 wherein authenticating is based on multiple characteristics of the anomaly region.
46. The method of claim 1 wherein the anomaly characteristic comprises anomaly severity.
47. The method of claim 46 wherein the anomaly severity represents an encoded data value.
48. The method of claim 1 wherein the digital medium is read by a reading device, and wherein monitoring further comprises recording prior settings of the reading device prior to reading; and restoring the prior settings of the reading device following authenticating.
49. The method of claim 48 wherein, following recording, the reading device is reset.
50. The method of claim 49 wherein, following recording, a cache on the reading device is reset.

51. The method of claim 48 further comprising selecting a data block size for the reading device.
52. The method of claim 48 further comprising disabling excessive retry attempts by the reading device.
53. The method of claim 48 further comprising reading locations of the digital medium known to be free of anomaly regions in order to archive a maximum transfer note.
54. The method of claim 48 further comprising ceasing reading when an anomaly location has been encountered.
55. The method of claim 48 further comprising storing the read data for statistical analysis.
56. A system for authenticating a digital medium comprising:
a monitor for monitoring a transfer rate of read data resulting from the reading of valid data stored on a digital medium at a physical location;
an anomaly detector for determining, from the monitored transfer rate, the presence of an anomaly region on the digital medium corresponding to the physical location of the valid data on the digital medium; and
an authenticator for authenticating the digital medium based on a characteristic of the anomaly region.
57. The system of claim 56 wherein the digital medium comprises an optical digital medium.
58. The system of claim 56 wherein the digital medium comprises a magnetic digital medium.
59. The system of claim 56 wherein the monitor monitors the transfer rate in real time, as the read data is read from the digital medium.

60. The system of claim 56 wherein the monitor monitors the transfer rate following reading of the read data from the digital medium.
- 5 61. The system of claim 56 further comprising an estimator for estimating the monitored data transfer rate and wherein the anomaly detector determines the presence of the anomaly region based on the estimated data transfer rate.
62. The system of claim 56 wherein the anomaly region causes a modification in the transfer rate of the read data.
- 10 63. The system of claim 62 further comprising a reading device for reading the valid data and wherein the modification in the transfer rate results from the reading device automatically initiating multiple retries of reading the valid data due to the presence of the anomaly region.
64. The system of claim 62 further comprising a reading device for reading the valid data and wherein the modification in the transfer rate results from the reading device automatically slowing down the reading the valid data due to the presence of the anomaly region.
- 20 65. The system of claim 56 wherein the anomaly region is located at a predetermined location on the medium.
66. The system of claim 65 wherein the predetermined location comprises an absolute address on the medium.
- 25 67. The system of claim 66 wherein the absolute address represents an encoded data value.

68. The system of claim 56 wherein the anomaly region is at a location on the medium that is analytically determined as a result of the step of determining the presence of the anomaly region.

5 69. The system of claim 68 wherein the predetermined location comprises an absolute address on the medium.

70. The system of claim 69 wherein the absolute address represents an encoded data value.

10 71. The system of claim 56 wherein the anomaly region comprises a first anomaly region and wherein the anomaly detector further:

determines, from the monitored transfer rate, the presence of a second anomaly region on the digital medium corresponding to a second physical location of second valid data on the digital medium; and

determines a relative location of the second anomaly region relative to the location of first anomaly region.

15 72. The system of claim 71 wherein the authenticator further authenticates based on the determined relative location.

20

73. The system of claim 71 wherein the second anomaly region is located at a predetermined location on the medium.

25

74. The system of claim 71 wherein the second anomaly region is at a location on the medium that is analytically determined as a result of the step of determining the presence of the second anomaly region.

75. The system of claim 71 wherein the relative location represents an encoded data value.

76. The system of claim 56 wherein the characteristic is the location of the anomaly region in the read data, and wherein if the location of the anomaly region in the read data matches the physical location of the anomaly region corresponding to the valid data, then the digital medium is determined as authentic.

5

77. The system of claim 76 wherein if the location of the anomaly region in the read data does not match the physical location of the anomaly region corresponding to the valid data, then the digital medium is determined as non-authentic.

78. The system of claim 56 further comprising a controller for controlling user access to the valid data on the digital medium based on whether the medium is authentic.

79. The system of claim 78 wherein controlling comprises one of allowing access, disallowing access, and limiting access to the valid data on the digital medium.

80. The system of claim 56 wherein the determination of the presence of the anomaly region results from a difficulty in the reading of the read data by a reading device.

81. The system of claim 56 wherein the anomaly region comprises a physical alteration of the digital medium that results in the valid data corresponding to the anomaly region being readable at a transfer rate that is different than a standard transfer rate of valid data not corresponding to the anomaly region.

82. The system of claim 81 wherein the physical alteration of the digital medium comprises a mechanical alteration.

83. The system of claim 81 wherein the physical alteration of the digital medium comprises an optical alteration.

84. The system of claim 81 wherein the physical alteration of the digital medium comprises a magnetic alteration.

85. The system of claim 56 wherein the authenticator reside in software code that is previously stored on the digital medium, prior to authentication.

86. The system of claim 56 wherein the anomaly detector and authenticator reside in firmware that is stored in a media drive performing the authentication or reside in a computing device controlling the media drive.

80. The system of claim 56 wherein a known characteristic of the anomaly region is previously stored, prior to authentication, and wherein authenticating the digital medium based on a characteristic of the anomaly region comprises comparing the characteristic to the known characteristic.

88. The system of claim 56 wherein the presence of the anomaly region is determined according to a modification in the transfer rate of the read data.

89. The system of claim 88 wherein the modification in the transfer rate comprises a reduction in the transfer rate and wherein the anomaly region is identified based on the extent of the reduction.

90. The system of claim 88 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant non-zero transfer rate.

91. The system of claim 90 wherein the resultant non-zero transfer rate results in a determination that the anomaly region is a genuine anomaly region.

92. The system of claim 88 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant zero transfer rate.

93. The system of claim 92 wherein the resultant zero transfer rate results in a determination that the anomaly region is a false anomaly region
- 5 94. The system of claim 93 wherein the false anomaly region indicates that the digital medium is non-authentic.
95. The system of claim 88 wherein the modification in the transfer rate comprises an increase in the transfer rate, and wherein the characteristic is determined based on the increase.
- 10 96. The system of claim 88 wherein the modification in the transfer rate comprises a response comprising an acceptable reduction in the data transfer rate followed by a sudden increase in the transfer rate to an increased transfer rate that is greater than a maximum transfer rate.
- 15 97. The system of claim 96 wherein the response indicates that an apparent anomaly region generated by an external source has been detected.
- 20 98. The system of claim 97 further comprising a filter unit for filtering the apparent anomaly region such that authenticating is not based on the apparent anomaly region.
99. The system of claim 56 wherein authenticating the digital medium is based on a characteristic of multiple anomaly regions.
- 25 100. The system of claim 56 wherein authenticating the digital medium is based on multiple characteristics of the anomaly region.
101. The system of claim 56 wherein the anomaly characteristic comprises anomaly severity.
- 30

102. The system of claim 101 wherein the anomaly severity represents an encoded data value.
103. The system of claim 56 further comprising a reading device for reading the digital medium, and wherein the monitor further records prior settings of the reading device prior to reading; and restores the prior settings of the reading device following authenticating.
104. The system of claim 103 wherein the monitor resets the reading device, following recording of the prior settings.
105. The system of claim 104 wherein the monitor resets a cache on the reading device is reset following recording of the prior settings.
106. The system of claim 103 wherein the monitor selects a data block size for the reading device.
107. The system of claim 103 wherein the monitor disables excessive retry attempts by the reading device.
108. The system of claim 103 wherein the monitor reads locations of the digital medium known to be free of anomaly regions in order to achieve a maximum transfer rate.
109. The system of claim 103 wherein the monitor ceases reading when an anomaly location has been encountered.
110. The system of claim 103 wherein the monitor stores the read data for statistical analysis.